HoGent

Faculteit 'Bedrijf en Organisatie'

Bluetooth Low Energy wearables in een Internet of Things cloud-infrastructuur met behulp van een smartphone als gateway

Jan Van Braeckel

Scriptie voorgedragen tot het bekomen van de graad
Bachelor in de toegepaste informatica

Promotor:
Joeri Van Herreweghe
Co-promotor:
Peter Leemans

Instelling: AllThingsTalk

Academiejaar: 2015-2016

Tweede examenperiode

Faculty 'Bedrijf en Organisatie'

Bluetooth Low Energy wearables in an Internet of Things cloud infrastructure using a smartphone as gateway

Jan Van Braeckel

Thesis submitted in fulfilment of the requirements for the degree of
Bachelor in applied computer sciences

Promoter:
Joeri Van Herreweghe
Co-promoter:
Peter Leemans

Affiliation: AllThingsTalk

Academic year: 2015-2016

Second exam period

Abstract

Preface

Contents

Chapter 1

Introduction

> "If you think that the internet has changed your life, think again. The IoT is about to change it all over again!"
>
> ———————————————
> Brendan O'Brien

The Internet of Things hasn't been around for a very long time, yet it's quickly becoming very popular and almost every tech company wants to be a part of it. It gained a lot of popularity around 2011 when IPV6 was released and it was around this time Gartner also took note of this trend and put it on their annual Hype Cycle for the first time. Around the same time of the growing popularity of the Internet of Things, the Bluetooth Special Interest Group released a new Bluetooth specification that was built for the Internet of Things: Bluetooth Low Energy. Gartner suggests that by 2020, around 20 billion 'things' will be connected to the Internet of Things, a market that Bluetooth Low Energy wants to play a big role in. This thesis aims to provide an introduction to Bluetooth Low Energy and how one would go about connecting Bluetooth Low Energy to the Internet of Things. In this chapter the problem that the thesis is trying to find an answer for is elaborated, as well as the actual questions that need answering. An introduction about 'AllThingsTalk' can also be found, a company that is trying to figure out how to connect Bluetooth Low Energy wearables with their Internet of Things infrastructure.

1.1 Problem statement and research questions

In this section, the goal is to quickly familiarize the reader with the subject this thesis is dealing about and which problems need to be solved in order to form a proper conclusion. First of all, the problem statement will be discussed where a quick sketch will be made as to why this thesis came to be. It will handle a subject that AllThingsTalk is very keen to discover for the development of their company and why combining Bluetooth Low Energy with their Internet of Things infrastructure is the next logical step for their business. Next, we'll look at the main question AllThingsTalk wants an answer for together with some smaller questions that logically follow it.

1.1.1 Problem statement

At the time of writing, there are already a lot of Bluetooth enabled products on the technology market. With the new Bluetooth Low Energy specification, Bluetooth is reaching out even further to products like socks[1], shoes[2], fitness bands[3] and more are being added to the list every day. The problem with these products is that in a lot of cases, the products only synchronize with a smartphone. Some manufacturers extend this connectivity by occasionally synchronizing the data the smartphone captures to their own proprietary cloud, where the data can be analyzed by both the company and the consumer. Most of the time, this is where the data cycle stops and it can't be further accessed by other parties, this is known as a closed loop system. In some cases, developers can still access the data with an API that communicates with the cloud service of the manufacturer, but this doesn't give any access to the raw sensor values and doesn't allow real-time data transfer. An example of a closed system versus open system can be found in figure 1.1.

On top of this, a lot of the devices being manufactured don't use standard SIG adopted BLE services, which makes interoperability with existing applications hard, if not impossible if authentication and encryption are added into the mix.

1.1.2 Research questions

There are a couple of questions that can be asked when combining Bluetooth Low Energy and the Internet of Things, and some of those questions alone could have multiple papers dedicated to them. For example, the matter of security will be a never ending debate, and even more concerns arise when talking about security in the Internet of Things. Another concern is privacy, but since this is very much a gray area,

---

[1]http://www.sensoriafitness.com/
[2]https://secure-nikeplus.nike.com/plus/products/basketball
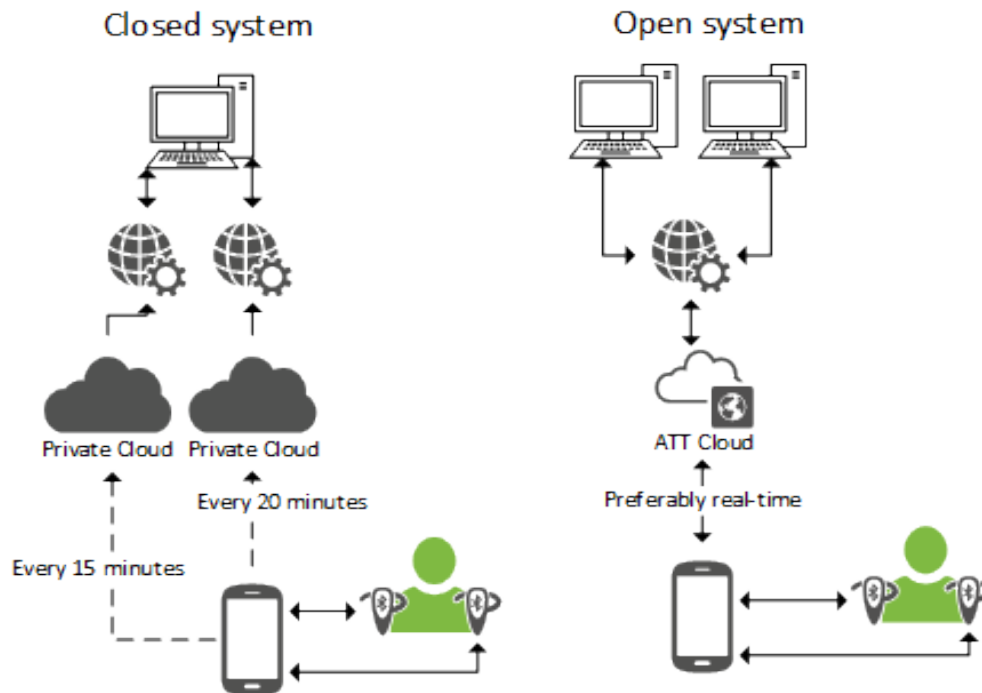[3]https://www.fitbit.com/

Figure 1.1: Image demonstrating a closed system (left) versus an open system (right). A closed system usually has its own (optional) cloud for every device from a different manufacturer, only pushing data but not pulling it. It also (not always) exposes a Web API to allow users to pull the data to their computer. An open system exposes *one* public cloud like the AllThingsTalk cloud with *one* Web API, also allowing 2-way data communication between smartphone and cloud.

it's hard to formulate a one-sided conclusion on this matter. Some of these concerns will be addressed further in section 9.2.

The main goals this thesis tries to fulfil are in essence very simple, but of course there are always some other questions that arise when looking at the big picture. These questions can be categorized as following, the questions in bold being the main research questions and the ones in plain text being auxiliary questions:

- **Can Bluetooth Low Energy wearables be used in an Internet of Things cloud infrastructure?**

- **Is is possible to use a smartphone as gateway to communicate with the AllThingsTalk cloud in real-time?**

- What is Bluetooth Low Energy?

- What is the difference between Bluetooth Low Energy and Bluetooth Classic?

- What are the pros and cons of this technology?

- What types of devices exist in Bluetooth Low Energy and how do they expose their data?

1.2 AllThingsTalk

As you've probably already noticed, the company AllThingsTalk has been referenced a couple of times in the previous section. The reason for this is that this thesis is affiliated with the company and is being written for them. The company helped shape the vision of the thesis and offered some very interesting insights and ideas for subjects to write about, subjects which were very interesting for their own use.

AllThingsTalk was founded in July 2013 and their main objective is to 'Make IoT ideas happen'. The company is already counting thirteen employees in two different countries, the headquarters being located in Ghent, Belgium. The office in Belgium counts seven people and is heavily focused on research & development engineering, project management and sales & marketing. The branch office is located in Belgrade, Serbia with the other six people, and their main focus is platform software development.

1.2.1 History

AllThingsTalk has come a long way since the start of the company. They've received multiple Research & Innovation grants from the government, the first being in September 2013 for building an open IoT platform: the AllThingsTalk Cloud. The second grant was received in May 2014, where the goal was to implement pattern recognition in their platform in order to help elderly people stay in their homes for a longer time. A third grant was acquired in February 2015, which was responsible for adding machine learning components to the platform.

Furthermore, they've hit some other major milestones throughout the years. In November 2014 they launched the first set of Rapid Development Kits for Internet of Things, where they added the Intel Rapid Development Kit in April 2015 and the LoRa Rapid Development Kit in November 2015. Other milestones include Internet of Things hackathons, the launch of IOTOPIA.be - a platform to introduce children in secondary schools to Internet of Things - and a LoRa partnership with Proximus, one of the largest telecommunications companies in Belgium.

Chapter 2

Methodology

> "Research is formalized curiosity. It is poking and prying with a purpose."
>
> —————————————————————————
>
> Zora Neale Hurston

This chapter aims to explain what approaches and methods were used in the making of this thesis. It explains what methods were used for the two major parts of this thesis, being the research & literature study and the Proof of Concept.

2.1 Research and literature study

Before starting the research, the most important question was 'what does AllThingsTalk already know?'. Of course, being a company revolving around Internet of Things, it wouldn't be much use to dedicate a large section of this paper to it. However, some research had to be done about Internet of Things in order to understand some core concepts and technologies that are used like transfer protocols such as MQTT and AMQP. A more abstract understanding was also needed, being how the Internet of Things works, what it's used for, why it's important and some more. This information is of course easily found online and wasn't of much use to include in this thesis.

That being said, the core subject of the research and literature study is about Bluetooth Low Energy. The research about this technology was done like you would research any other subject. Initially, the plan was to rely heavily on the official documentation of Bluetooth, but since the complete Bluetooth specification is over 2000 pages in length, a more practical approach was to purchase books that explain Bluetooth Low Energy, two of them being REFERENTIE BOEK 1 and REFERENTIE BOEK 2.

There are also training videos to be found on the Bluetooth website as well as various other short introductions to the technology all over the web, which provide a

basic and quick understanding about the technology.

2.2   Proof of Concept

You don't get to know something without actually trying it out, which was one of the biggest focuses of the Proof of Concept. The actual goal of the Proof of Concept was more to provide the Bluetooth Low Energy layer than to connect to the Internet, as AllThingsTalk provides easy-to-use libraries in various language to connect to their platform.

In order to help speed up the learning process and quickly allow me to prototype and try out the technology, various devices were provided which offer a range of Bluetooth Low Energy profiles, services and characteristics, these terms are explained further in chapter 6. These devices will shortly be introduced in chapter 8.

The first goal of the Proof of Concept was to connect to a Bluetooth Low Energy device and read data on a smartphone. Various examples and repositories with source code provided some interesting insights as to how this API worked. Bluetooth also offers some starter kits to kickstart any project that wants to use Bluetooth Low Energy, including a very comprehensive and easy to use wrapper around the Android Bluetooth API.

Further goals of course include writing data and coupling the Bluetooth layer to the network layer, automatic service discovery and mapping, automatic generation of assets on the online platform and more. The most important concepts on how to do this are elaborated in chapter 8 and the accomplishments are listed in the conclusion, section 9.1.

Chapter 3

Bluetooth Low Energy

> "Bluetooth Low Energy is going to
> change the way the world connects."
>
> Robin Heydon

Bluetooth has been around for a long time, and with the release of technologies like NFC it seemed like Bluetooth wasn't going to last for much longer. However, Bluetooth Low Energy has breathed new life into Bluetooth and it's now more popular than ever. Originally known as Wibree by Nokia, it was later merged into the Bluetooth standard after much consideration. This technology was built from the ground up to be as energy efficient as possible and will power the Internet of Things for years to come. Exciting updates are also on the way like mesh networking, allowing different nodes in a network to relay data to one another. In this chapter we'll be looking at what Bluetooth Low Energy actually is, what the key differences are between Bluetooth BR/EDR and Bluetooth Low Energy. Also worth investigating are the limitations of Bluetooth Low Energy and how this technology achieves low energy like no other.

3.1   What is Bluetooth Low Energy

In essence, Bluetooth Low Energy is the first open standard that consumes extremely low power. It has been built from scratch and has more things not in common than it does with Bluetooth, so the name can be a little bit confusing. Every component in this specification has been designed to consume as little power as possible, that's why this technology can also be called a 'Coin cell' technology. This because a Bluetooth Low Energy enabled device can (theoretically, with normal usage) achieve battery life of around eight months on a coin cell battery. A great example of this are beacons, which can achieve a very long battery life if configured correctly. If fitted with a bigger battery, it can last for over two years. More information about the battery usage and how this low energy is achieved can be found in section 3.4.

However, you might be thinking: if Bluetooth Low Energy is so great, why isn't it replacing other wireless technologies? The main reason for this is because it's very slow and has very little range. A couple of other limitations are present, but these will be more closely looked at in subsecion 3.2.2. Bluetooth Low Energy's main use is intended for Personal Area Networks, with a gateway in range that can relay data to a cloud service in order to connect various devices to the internet.

3.2   Key differences between classic Bluetooth

As the diligent reader probably already noticed, it seems that Bluetooth and Bluetooth Low Energy are worlds apart from one another. This is in fact very correct so it's hard to just list some differences and be done with it. In the next two subsections we'll look at why Bluetooth Low Energy is completely different from Bluetooth and should be seen as a new technology in its whole instead of an enhancement to the existing Bluetooth. The key limitations of the Bluetooth Low Energy specification are also addressed further in subsection 3.2.2.

3.2.1   A new technology emerges

A lot of authors are looking to compare Bluetooth with Bluetooth Low Energy, but this is an unfair comparison since the use cases for both of these technologies are completely different. As the name suggests, Bluetooth Low Energy is marketed for low energy devices like wearables and sensors, so it isn't here to replace other wireless technologies in the slightest where a continuous flow of data is required. They've also both been built around completely different core principles and have been designed to fulfil these requirements as best as possible.

3.2.2   Limitations of Bluetooth Low Energy

Bluetooth Low Energy doesn't bring all good news, but there are also a few key limitations to the technology, as with everything in life. Because the technology uses very little power, it's fairly easy to understand that the transmit power and transfer speeds aren't anywhere near other wireless technologies. In theory, Bluetooth Low Energy can achieve ranges of up to 65 meters and upcoming updates to the specification prove that this range will be increased even more. However, most manufacturers won't want their peripheral to transmit at such high range, because this will cause increased battery usage in turn. In practice, this range is of course much lower, as walls and even humans wreak havoc on the transmission of data.

Another limitation is the transfer speed. Again, in theory, Bluetooth Low Energy can have a (full packet) transfer speed of up to 1 Mbps[1]. If you take into account the actual data contained in said packet and add up all of the overhead that goes into transferring a packet, 5 to 10 KB per second is a much more realistic representation. Knowing this, it's safe to assume that Bluetooth Low Energy won't be replacing WiFi any time soon.

3.3   Bluetooth configurations

Bluetooth Low Energy is known by a variety of names on the market and while some of them are used to describe the same technology, in a few there's some differences to be found. 'Bluetooth Low Energy' is mostly used as a catch-all name and can consist of a few different configurations. Some people assume 'classic' or Bluetooth BR/EDR is also Bluetooth Low Energy, but this assumption couldn't be more wrong. If you have a product that specifies that you must have Bluetooth Version 4.0 or later, you're probably dealing with a Bluetooth Low Energy product.

Other names that can commonly be found are Bluetooth Smart (single-mode) and Bluetooth Smart Ready (dual-mode), these are both specifications of Bluetooth Low Energy but have one key difference between each other: backwards compatibility. Bluetooth Smart has been designed to only allow interoperability between itself and Bluetooth Smart Ready products. You'll usually see this configuration in wearable devices that connect to a smart phone, in this case the wearable is a Bluetooth Smart product and the smartphone is a Bluetooth Smart Ready product. Bluetooth Smart Ready on the other hand has been designed to allow communication with Bluetooth, Bluetooth Smart Ready and Bluetooth Smart products. Bluetooth Smart Ready is commonly present in the most recent smartphones, which will allow communication with Bluetooth products like headphones but also Bluetooth Smart products like a

---

[1]1 Mbps equals to 100 kilobytes per second.

Table 3.1: Compatibility table of Bluetooth specifications

Bluetooth specification	*Supports BR/EDR*	*Supports BLE*
Pre-v4.0	v	x
4.x Bluetooth Smart	x	v
4.x Bluetooth Smart Ready	v	v

smart band. A more comprehensible and orderly overview of these technologies can be found in table 3.1.

3.4   How low energy is achieved

There are a couple of techniques Bluetooth Low Energy uses to achieve low energy consumption. The fact alone that it can run off a 3 volt CR2032 coin cell battery and still retain 8 months of battery life proves that it is indeed a *true* low energy technology. There are a couple of decisions that made it possible to achieve this low amount of energy consumption, some being the following:

- **Use the radio as little as possible.** Keeping the radio on any wireless technology active requires quite a bit of power, which is also the case with Bluetooth Low Energy. By using the radio as little as possible, Bluetooth Low Energy can significantly increase its battery life. At a set interval, devices will broadcast advertising packets on the three advertising channels, which are explained more in section 5.2. After it advertises, it must listen briefly to any connection requests that follow it, in between these events the radio is simply turned off. The radio and the protocol stack, explained more in depth in chapter 4, have also been designed to be as fast as possible. An advertising event, connection event, reading a single value of data and acknowledging the event can take as little as 3 milliseconds, which is vital in not only keeping the energy consumption to a minimum, but it also helps passively cool the radio.

- **Keep packets very small.** Restricting the packet length to a maximum of 47 bytes allows very rapid packet transfers, which in turn contributes to keeping the radio off as much as possible. A maximum size packet of 47 bytes can be transferred in as little as 0.3 milliseconds. Keeping packets small also lowers the complexity of the transmitter and receiver, resulting in much lower power consumption than technologies that allow large packets.

Chapter 4

The Bluetooth Low Energy protocol stack

4.1 Controller

4.1.1 Physical Layer

4.1.2 Link Layer

STATE MACHINE https://www.bluetooth.com/specifications/bluetooth-core-specification/technical-considerations

4.1.3   Host Controller Interface

4.2   Host

4.2.1   Host Controller Interface

4.2.2   Logical Link Control and Adaption Protocol

4.2.3   Attribute Protocol

4.2.4   Security Manager Protocol

4.2.5   Generic Access Profile

4.2.6   Generic Attribute Profile

4.3   Application

4.3.1   Application

Chapter 5

Generic Access Profile

> "I NEED TO LOOK UP A QUOTE
> FOR THIS CHAPTER"
>
> ———————————————————
> Jan Van Braeckel

One of the most important parts in Bluetooth Low Energy, if not most important one, is the Generic Access Profile. This profile determines everything from advertising device presence to continuing to a connection. It specifies rules how devices can and must behave in order to interact with one another and imposes some general rules both devices have to follow. It also supports some modes and procedures to secure the data link, like authentication, bonding, authorization and encryption. In this chapter, we'll look at some general information about the Generic Access Profile like device roles and data channels before taking a look at how advertising, scanning, broadcasting and connections work.

5.1 Roles

Every Bluetooth Low Energy device has a one or more roles it can fulfil. Each of these roles have been optimized to perform their task as best it can. First of all there's the Broadcaster role, which only requires a device to have a transmitter and advertising profile. Broadcasters aren't necessarily devices that you can connect to, so manufacturing broadcast only devices could cut down on cost even more as there's no need to have a receiver on these devices. An example of this is a thermostat which constantly broadcasts its temperature.

Secondly there's the Observers, these devices are opposite to broadcasters as they don't require a transmitter. Observers just listen to advertising events and process the data further, without ever making a connection. These devices make perfect gateways for Observers, as a connection will never occur between these two, and the observer can just relay the data to an other collection point.

The last two types of roles are Peripherals and Centrals. These two are the most complex roles as both devices are required to have both a transmitter and receiver. The big difference however is that a Peripheral will always act as a slave in a connection and a Central will always act as a master. This also means that the peripheral will (most of the time) be the least powerful device with the lowest battery life, like a watch or a sensor. It's vital that Peripheral devices don't do the heavy lifting in connections because this would drain the battery too quickly. The Central in a connection is usually a much more powerful device with a better battery life, like a smartphone, tablet or even computers.

5.2 Data channels

Bluetooth Low Energy uses a number of channels in the 2.4 GHz ISM frequency band. Some of these channels are used for advertising and most of them are used for transferring data once a connection has been made. In total 40 channels are used, 3 of which are used for advertising and the remaining 37 are used for connections. The frequency range starts at 2402 and ends at 2483.5, giving each frequency a range of about 2 MHz to operate on. These channels have been carefully picked to have the least interference possible from WiFi on the advertising channels. Since every connection starts with advertisements it's vital that these packets flow without interference. A visualization of these channels can be found in figure 5.1.

In order to make sure that connection packets flow as frequently as possible without having too many dropped packets, Bluetooth Low Energy uses adaptive frequency hopping. This means that at a set interval that the master and slave negotiate with each other, they will switch frequency with a known algorithm, ensuring they'll always end up in the same frequency band. If data doesn't make it through on a given channel,

the frequency hop will occur prematurely and both master and slave will move on to the next frequency and resend the packet(s) that weren't acknowledged.
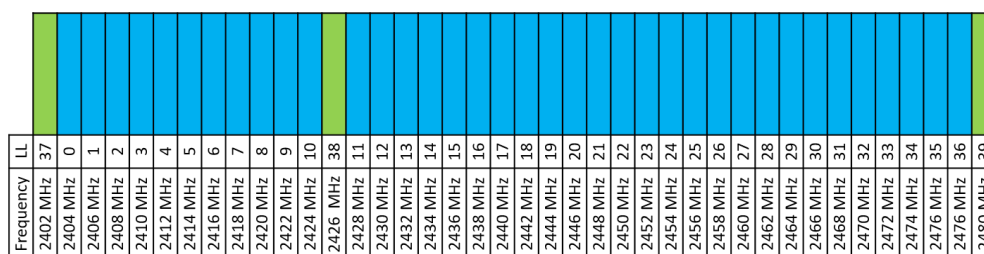

Figure 5.1: Image visualizing the Bluetooth Low Energy channel spectrum. The green channels are advertising channels while the remaining 37 are used for connections. LL stands for the corresponding number that the link layer assigns to these channels.

5.3   Advertising

As quoted a few times before, advertising is one of the most important procedures in Bluetooth Low Energy. A device can be built solely around advertising data, but no device can work without it. Its main purpose is to broadcast the device is present and active so devices can connect with it if the device is connectable, but it can be used for more than that. A typical device will constantly be advertising its state to other devices. This state can be device name, device address and even an (incomplete) list of available services on the device. The advertising interval differs from device to device, but it's easy to conclude that a device with a faster advertising interval will drain battery more quickly than one with a slow advertising interval.

If the device can't fit enough data into the advertising packet, there is a second option to send more data without requiring a connection. Once a device receives an advertising packet, it can send out a Scan Request, acknowledging that it received the previous advertising packet and is listening for extra packets if there are any. The peripheral can then proceed to send a Scan Response with extra data. It's important to note however that a peripheral that uses Scan Requests isn't connectable, which means that it's perfect for a beacon or any sort of other advertising device. SOURCE

5.3.1   Data format

As discussed in subsection 4.1.2, each packet, be it advertising or data, has the same maximum length and structure but the data part of the packet is filled depending on the type of packet that is sent. The data in an advertising packet is filled with AD Types which take up one byte, and the data for that AD Type which is of variable

length. An incomplete list of these AD Types together with their definition is found below. A full list of AD Types together with their descriptions can be found on the Bluetooth website[1] and Bluetooth Core Specification.

- List of Service Class UUIDs (0x02 - 0x07): Helps with finding out the purpose of a device, can contain a complete or partial list of available services on the device.

- Shortened or Complete Local Name (0x08 & 0x09): Usually gives a friendly name to a device in UTF-8 format.

- Service Data (0x16): Represents a GATT service and the data associated with it, this is in essence how a broadcasting only device transfers data.

- Appearance (0x19): Contains a number representing the external appearance. This can be anything from "Generic Keyring" to "Joystick".

- Indoor Positioning (0x25): Helps with mapping BLE devices in a building, can contain coordinates, altitude, floor number and location name.

- Advertising Interval (0x1A): How often the device advertises its presence.

5.4   Broadcasting

As discussed in the Advertising section (5.3), it's possible to have a device that only advertises data and isn't connectable, or its main purpose doesn't rely on connections. This is known as a broadcast device and can be used in broadcasting network topologies. Take for example a radio station, it simply broadcasts its data and it doesn't really matter how many people are listening. When broadcasting, you don't care how many devices can be listening to your data and you shouldn't care about security when advertising data. A great example of this are beacons, which broadcast a very simple payload telling they're there. Infinite amount of devices can listen in on this data communication and use it for their own. Once you need to send sensitive data or only want two-way communication, a connection must be established which uses the GATT Profile to exchange data between master and slave. More information on GATT can be found in chapter 6.

---

[1]https://www.bluetooth.com/specifications/assigned-numbers/generic-access-profile

5.5 Connections

Once a central is ready to connect to a peripheral, it sends a connection request to the peripheral. The peripheral can then accept or deny the request and once accepted, the connection sequence can begin. During the establishment of a connection, a few key rules are established that will stay in place for the remainder of that connection or until both devices agree to change the connection parameters. These rules can be hop frequency, hop amount, what to do when the connection fails and more. Some of these parameters can be changed during the connection lifetime, an example of this is given in section 5.2, where the devices can agree to avoid a given channel for a certain time because there's too much interference. Once a connection has been established, the peripheral will stop advertising its presence since it can only be connected to one central. For the remainder of that connection, both master and slave will exchange data solely with GATT until the connection terminates. The peripheral will then continue once again to advertise its presence.

Chapter 6

Generic Attribute Profile

"You can have data without
information, but you cannot have
information without data."

Daniel Keys Moran

At the core of Bluetooth Low Energy communication, the Generic Attribute Profile or GATT is something a client will use in every data request or data push once a dedicated connection has been set up. It defines the way data is transferred in Bluetooth Low Energy and it uses the Attribute protocol, which is the protocol that stores Services, Characteristics, Descriptors and their respective values. In this chapter the general Attribute Profile and Protocol will be discussed, as well as the different data structures that come in to play. An example of an Attribute server will also be given using a standard SIG-approved Profile, as well as why and how one would implement their own Profile, either because the SIG-approved Profiles don't fit the use case or because the manufacturer wants to make the used technology more private.

6.1 Profiles

Profiles in Bluetooth Low Energy are an abstract representation of how a device can be implemented to fill a specific use case. These profiles are purely an example of how things can be done and these can be extended as you want or you can start from scratch and define your own profile. The Heart Rate profile for example defines that the device uses a minimum of two services: the Heart Rate Service and the optional Device Information Service. Its role is a Heart Rate Sensor and it serves as a collector, collecting data and then broadcasting it or sending it to a connected master device.

6.2 Services

All data in Bluetooth Low Energy is accessed through services. You can compare it to simple Object Oriented principles: a service has multiple characteristics and a characteristic belongs to one single service. An example of this is the Bluetooth SIG defined Heart Rate Service. This document defines the way the Heart Rate Service is used and what characteristics are contained in the service. For example, the Heart Rate Service defines 3 characteristics: Heart Rate Measurement, Body Sensor Location and Heart Rate Control Point, only the Heart Rate Measurement is mandatory to include.

A device can host any number of services which are independent of one another. Every service also has its own security options which you can customize. You can set options like encryption for individual services or the device as a whole.

Apart from multiple primary services, a service can also be contained in a parent service, this is then known as a secondary service. However, the secondary service system isn't encountered that often, but it can be useful at times. Take for example a device which has two temperature sensors, one for the outside temperature and one for the battery temperature. The manufacturer could then choose to include the temperature service for the battery as a secondary service of the battery service, this avoids ambiguity.

Apart from the SIG-defined services, a custom service can be designed if the defined services don't meet the expectations of the use case. It's up to the manufacturer to provide documentation for these services or not.

6.3 Characteristics

The actual data of services is contained in characteristics. Every characteristic belongs to a specific service and has a value attached to it. However, it's not because you can see the characteristic, that you don't need special rights to read or write it. A characteristic can specify certain rights like read, write, read uncommitted (where no

acknowledgement is sent for the write request) and more. This is something that can be ignored, but an error message will be returned anyway if you try to read a characteristic that isn't readable. These permissions can be used to notify the user interface that it shouldn't allow the user to interact with certain characteristics.

If we take our trusty Heart Rate for example, the Heart Rate Measurement, we can look at the data structure and how the value should be parsed. This characteristic also has some "Flags" bits which indicate things like the data type of the value (UINT8 or UINT16) and if certain fields are present or not. Depending on the Flags, there are a couple of values to be found inside this characteristic: Heart Rate Measurement Value, Energy Expended and RR-Interval.

As with services, custom characteristics can also be defined. A template characteristic can be used or the bit structure can be designed from the ground up to accommodate the specific use case.

6.4   Descriptors

If we go down even further, we come to the descriptors. These can optionally accompany characteristics and describe the value of a given characteristic. The descriptors can house very useful data like a description, a valid range of the data and a couple more. If these descriptors are defined, it can greatly help with building up a user interface by only allowing certain values or showing a description for a custom made characteristic, but one shouldn't rely on these descriptors as they're not filled in more often than not.

Chapter 7

Why Bluetooth Low Energy and Internet of Things

> "I NEED TO LOOK UP A QUOTE FOR THIS CHAPTER"
>
> Jan Van Braeckel

The Internet of Things is quickly growing and it's already huge, filled with both long-range sensors using LoRa and Sigfox technologies and short-range sensors using WiFi or directly connected with a gateway connected to internet. Why would it then be beneficial to add another spectrum of devices: Bluetooth Low Energy? The main reason for this is because no other technology fills this spectrum of devices yet. Right now, you can compare wireless IOT technologies against 2 axis: power and range, as seen in figure 7.1. Before Bluetooth Low Energy, there wasn't really any major technology to fill the Low Energy, Low Range spectrum. One can say that Zigbee or other technologies could fill this end of the spectrum, but none of these are as widely adopted as Bluetooth Low Energy is today. In this chapter we'll further discuss the use cases Bluetooth Low Energy can fulfil in this Low Power, Low Range spectrum as well as briefly introducing its competitors, before ending with what the future holds for Bluetooth Low Energy.
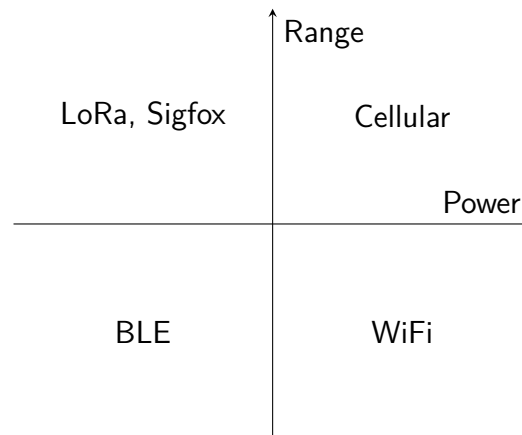
Range

LoRa, Sigfox   Cellular

Power

BLE   WiFi

Figure 7.1: Image showing Bluetooth Low Energy's place in the Range vs Power spectrum.

7.1   Uses of Bluetooth Low Energy

When looking at the adopted Bluetooth Low Energy profiles and services, as discussed in sections 6.1 and 6.2, it's quite easy to find some general use cases that the technology can be used for. Some important use cases are listed below, but are surely not limited to this list:

- **Quantified Self, Sport and Fitness**: Cycling Power, Cycling Speed and Cadence, Running Speed and Cadence, Body Composition, Heart Rate, Weight Scale

- **Health care**: Blood Pressure, Glucose, Continuous Glucose Monitoring, Health Thermometer, Heart Rate and Weight Scale, Pulse Oximeter

- **Location and Proximity**: Find Me, Location and Navigation, Proximity, Indoor Positioning

Of course, once we include non-adopted specifications, the list could go on forever with entries being added every day. For example, there's the "Flower Power"[1] device which measures your plant health by monitoring air temperature, soil temperature, soil moisture, soil electrical conductivity and more. It synchronizes with a smartphone that has the Flower Power application paired to the device and synchronizes the data to an online cloud at set intervals, where the data can then be queried with an API (closed system as seen in figure 1.1). A lot of these services aren't included in the adopted specifications, so extending standard Bluetooth profiles with your own can greatly

---

[1]http://www.parrot.com/usa/products/flower-power/

expand the possibilities of the technology. However, if the manufacturer doesn't release the specifications of their device, interoperability with existing apps or integrating that device in other apps will be made very hard.

However, the Flower Power example isn't exactly the best Bluetooth Low Energy use case in existence. For example, what if there's a gardener who plants some of these devices in his/her customers' yards. If the customer isn't home for two weeks, then there's no cellphone to synchronize the data to and the gardener will have to come over to check if the plants need care either way. Some people in the community also thought this was a problem and made a NodeJS gateway application to run on a Raspberry PI or other computer but the product wasn't originally designed for this and the NodeJS gateway leaves a lot to be desired.

7.2 Competitors

As the rules of marketing tell us, there aren't (or there are very little) products that have no significant competitors. While Bluetooth Low Energy is trumping its competitors pretty well, it's still worthwhile to look at the these other technologies and what they do.

7.2.1 ZigBee

ZigBee has been designed from the ground up with automation in mind, as well as Internet of Things. It's not just focused on home automation, but it's also used for smart energy products, health care, equipment monitoring, remote controls and more. Some major technology manufacturers have adopted this technology and are selling home automation kits for people to set up in their homes, like Xiaomi with its Smart Home kit. Another thing ZigBee does very well is mesh networking. Devices can be connected with one another and exchange data without needing additional gateways to fetch the data. However, the problem with ZigBee is that the platform is completely open and changes can be made for it as the manufacturer wishes. So it might happen that two devices with a ZigBee chip aren't even able to communicate with one another.

7.2.2 Z-Wave

Another wireless technology that is built completely for home automation is Z-Wave. The major difference between ZigBee and Z-Wave however, is that the Z-Wave technology isn't open. This is both good and bad because it's not open at all to development, you simply take the technology as it comes and no flexibility is offered beyond that point. For the consumer this is beneficial however, ensuring interoperability between Z-Wave devices, since Z-Wave also features mesh networking.

7.2.3 ANT

ANT is another good example of a Bluetooth Low Energy competitor. This is again a proprietary technology and was built with sensor networks in mind. It features powerful mesh networking as well as star, tree and point-to-point networks, allowing all kind of networks to be used in unison.

7.3 Other wireless technologies

There are loads of other technologies that can be used to power the Internet of Things, but we won't go too much in depth in these. Some of these technologies and protocols are X10 (home automation), KNX (home automation) and M-bus (industry). Other very big technologies, not necessarily in the Low Energy/Low Range spectrum are LoRa (Long Range), GPRS (cellular) and Sigfox (Long Range).

7.4 Future of Bluetooth Low Energy

Bluetooth Low Energy has been an exciting technology from the start and is gaining popularity at a very rapid rate. While the Bluetooth 4.0 specification brought Bluetooth Low Energy to life, some very much needed updates have made it to the Bluetooth specification, which is now at version 4.2. Bluetooth 4.1 brought improved consumer usability with better co-existence between Bluetooth Low Energy and Bluetooth BR/EDR, as well as increased data exchange rate and more flexibility for the developers. The 4.1 specification also brought IP-based connections to Bluetooth Low Energy. In essence, a device can directly communicate over internet once it's been connected to a gateway that has internet access, like a smartphone.

The newest update, Bluetooth 4.2, brings yet more changes to the Bluetooth specification. It brings improved speeds yet again, support for IPv6, 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) and improved security.

The Bluetooth SIG is constantly working on Bluetooth Low Energy, and it has been announced that the range would be significantly improved. They also brought mesh networking to the table, just like ZigBee, Z-Wave and ANT. These improvements will bring even more use cases to Bluetooth Low Energy, the main one being home automation.

Chapter 8

Android programming

Chapter 9

Discussion

9.1   Conclusion

9.2   Concerns

A more concerning limitation is that Bluetooth Low Energy operates in the 2.4 GHz ISM frequency band, the same band that WiFi uses. They've chosen this band because the 2.4 GHz ISM band doesn't require any licensing cost, contributing to the very low chip cost of Bluetooth Low Energy devices. Luckily, Bluetooth Low Energy features an excellent algorithm to avoid major interference from WiFi, as it will avoid any channel that is being heavily used by other technologies.

9.3   Future work

Bibliography

List of Figures

List of Tables